

Jonathan M. Lebe, State Bar No. 284605
Jon@lebelaw.com
Zachary T. Gershman, State Bar No. 328004
Zachary@lebelaw.com
Nicolas W. Tomas, State Bar No. 339752
Nicolas@lebelaw.com
Lebe Law, APLC
777 S. Alameda Street, Second Floor
Los Angeles, CA 90021
Telephone: (213) 444-1973

Attorneys for Plaintiff Cindy Villanueva,
Individually and on behalf of all others similarly situated

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

Cindy Villanueva, individually and on
behalf of all others similarly situated,

Plaintiff,

vs.

UKG, Inc.,

Defendant.

CLASS ACTION COMPLAINT FOR:

1. Negligence;
2. Breach of Contract;
3. Violation of the CCPA (Cal. Civ. Code § 1798.150, *et seq.*);
4. Violation of the CRA (Cal. Civ. Code § 1798.80, *et seq.*);
5. Violation of the Right to Privacy (Cal. Const., art. I § 1); and
6. Violation of the Unfair Competition Law (Cal. Bus. & Prof. Code § 17200, *et seq.*).

DEMAND FOR JURY TRIAL

Plaintiff Cindy Villanueva (“Plaintiff”), individually and on behalf of others similarly situated, alleges as follows:

NATURE OF ACTION AND INTRODUCTORY STATEMENT

1. Every year millions of Americans have their most valuable personal information (“PI”) stolen and sold online because of unauthorized data disclosures. Despite the dire warnings about the severe impact of unauthorized data disclosures

1 on Americans of all economic strata, companies still fail to put adequate security
2 measures in place to prevent the unauthorized disclosure of private data about their
3 customers or potential customers.

4 2. Defendant UKG, Inc., known as Ultimate Kronos Group,
5 (“Defendant”) is a multinational technology company providing payroll,
6 timekeeping, and human resource services to companies and businesses nationwide
7 using its software including, “Kronos Private Cloud” and “UKG Workforce
8 Central.” Defendant provides its services to thousands of large employers, who in
9 turn, have millions of end-users. Defendant is one of the largest, if not the largest,
10 provider of workforce management services to major employers. In doing so,
11 Defendant collects the most sensitive and confidential PI of millions of users of its
12 software.

13 3. Through its software, Defendant provides services to employers to
14 assist in tracking employee’s hours, pay, and time records. In doing so, Defendant
15 retains sensitive information related to payroll records such as direct deposit
16 information, bank account information, addresses, and social security numbers,
17 among other things.

18 4. As a corporation doing business in California, Defendant is legally
19 required to protect PI from unauthorized access and exfiltration.

20 5. On or around December 11, 2021, Defendant’s cloud-based time and
21 attendance systems, including “Kronos Private Cloud” and other UKG systems
22 were exploited by hackers through a ransomware attack causing a massge outage
23 of their payroll system and exposing millions of worker’s information to
24 cybercriminals as a result of Defendant’s failure to equip its system with reasonable
25 and adequate security.

26 6. On December 13, 2021, Defendant’s Executive Vice President, Bob
27 Hughes made the following announcement on Defendant’s website:

28 “We are reaching out to inform you of a cyber security incident that has
disrupted the Kronos Private Cloud.

As we previously communicated, late on Saturday, December 11, 2021, we became aware of unusual activity impacting UKG solutions using Kronos Private Cloud. We took immediate action to investigate and mitigate the issue, and have determined that this is a ransomware incident affecting the Kronos Private Cloud—the portion of our business where UKG Workforce Central, UKG TeleStaff, Healthcare Extensions, and Banking Scheduling Solutions are deployed. At this time, we are not aware of an impact to UKG Pro, UKG Ready, UKG Dimensions, or any other UKG products or solutions, which are housed in separate environments and not in the Kronos Private Cloud.

We are working with leading cyber security experts to assess and resolve the situation, and have notified the authorities. The investigation remains ongoing, as we work to determine the nature and scope of the incident.

We deeply regret the impact this is having on you, and we are continuing to take all appropriate actions to remediate the situation. We recognize the seriousness of this issue and will provide another update within the next 24 hours.”¹

7. Though this unauthorized data breach impacted millions of workers, many workers affected by the breach did not find out about the breach from Defendant, but instead found out about it through public postings such as the one above, from news outlets, or from their employer. To date, many workers are still in the dark as to what type of PI was compromised by this breach, because Defendant has yet to provide legally compliant notice to those impacted of the breach to those impacted.

8. More recently, on March 4, 2022, Defendant made the following update regarding the data breach:

“Our forensic investigation is now complete. As previously communicated, the investigation determined that the personal data of individuals associated with two of our customers was exfiltrated as a result of the incident. Both affected customers have been notified, so if you have not heard from us directly, you can feel confident that we have found no evidence that any personal data of individuals associated with your organization was

¹ UKG Workforce Central – Leo Daley, https://community.kronos.com/s/feed/0D54M00004wJKHiSAO?language=en_US (last visited Mar. 10, 2022).

1 exfiltrated.”²

2 9. On information and belief, Defendant has not provided legally
3 compliant notice to the millions of workers whose information was not only
4 exfiltrated, but also unlawfully disclosed and accessed as a result of the breach. To
5 date, Defendant has not confirmed what type of PI was accessed, disclosed, stolen,
6 or exfiltrated.

7 10. As a result of Defendant’s failure to provide reasonable and adequate
8 data security, Plaintiff’s and putative class members’ PI has been exposed to those
9 who should not have access to it. Plaintiff and putative class members are now at
10 much higher risk of identity theft and for cybercrimes of all kinds, especially
11 considering the highly valuable and sought-after PI stolen here—financial
12 information relating to millions of worker’s payroll records.

13 11. In addition to the privacy implications, the resulting data breach
14 massively disrupted payroll systems for many large companies that use
15 Defendant’s payroll services, including many grocery stores, insurance companies,
16 hospitals, department stores, food manufacturers, and a plethora of other businesses
17 who rely on Defendant’s services for processing their employee’s payroll
18 information. This massive disruption of Defendant’s payroll and timekeeping
19 system resulted in many workers being paid late, being paid incorrectly, or not
20 being paid at all during the holiday season and during the Covid-19 pandemic.

21 12. Defendant’s Privacy Policy specifically states that it limits access of
22 PI and data only to those “who have a specific business purpose for maintaining
23 and processing such information.” Despite this claim, and other claims in its
24 privacy policy, Defendant allowed its system to be attacked and exploited by
25 hackers, resulting in a massive breach of critical PI of millions of end-users off its
26 payroll system.

27 13. The PI exposed by Defendant as a result of its inadequate data security

28 ² UKG Kronos Private Cloud Status Updates Archives,
<https://www.ukg.com/KPCupdates/Archive> (last visited Mar. 10, 2022).

1 is highly valuable on the black market to phishers, hackers, identity thieves, and
2 cybercriminals. Stolen PI is often trafficked on the “dark web,” a heavily encrypted
3 part of the Internet that is not accessible via traditional search engines. Law
4 enforcement has difficulty policing the dark web due to this encryption, which
5 allows users and criminals to conceal identities and online activity.

6 14. When malicious actors infiltrate companies and copy and exfiltrate the
7 PI that those companies store, or have access to, that stolen information often ends
8 up on the dark web because the malicious actors buy and sell that information for
9 profit.

10 15. The information compromised in this unauthorized data breach
11 involves sensitive payroll information which is significantly more valuable than the
12 loss of, for example, credit card information in a retailer data breach because, there,
13 victims can cancel or close credit and debit card accounts. Whereas here, the
14 information compromised is difficult and highly problematic to change—driver’s
15 license numbers, social security numbers, addresses, and banking information.

16 16. Once PI is sold, it is often used to gain access to various areas of the
17 victim’s digital life, including bank accounts, social media, credit card, and tax
18 details. This can lead to additional PI being harvested from the victim, as well as
19 PI from family, friends, and colleagues of the original victim.

20 17. Unauthorized data breaches, such as these, facilitate identity theft as
21 hackers obtain consumers’ PI and thereafter use it to siphon money from current
22 accounts, open new accounts in the names of their victims, or sell consumers’ PI to
23 others who do the same.

24 18. Federal and state governments have established security standards and
25 issued recommendations to minimize unauthorized data disclosures and the
26 resulting harm to individuals and financial institutions. Indeed, the Federal Trade
27 Commission (“FTC”) has issued numerous guides for businesses that highlight the
28 importance of reasonable data security practices. According to the FTC, the need

1 for data security should be factored into all business decision-making.³

2 19. In 2016, the FTC updated its publication, Protecting Personal
3 Information: A Guide for Business, which established guidelines for fundamental
4 data security principles and practices for business.⁴ Among other things, the
5 guidelines note businesses should properly dispose of personal information that is
6 no longer needed, encrypt information stored on computer networks, understand
7 their network's vulnerabilities, and implement policies to correct security
8 problems. The guidelines also recommend that businesses use an intrusion
9 detection system to expose a breach as soon as it occurs, monitor all incoming
10 traffic for activity indicating someone is attempting to hack the system, watch for
11 large amounts of data being transmitted from the system, and have a response plan
12 ready in the event of the breach.

13 20. Also, the FTC recommends that companies limit access to sensitive
14 data, require complex passwords to be used on networks, use industry-tested
15 methods for security, monitor for suspicious activity on the network, and verify
16 that third-party service providers have implemented reasonable security measures.⁵

17 21. Highlighting the importance of protecting against unauthorized data
18 disclosures, the FTC has brought enforcement actions against businesses for failing
19 to adequately and reasonably protect PI, treating the failure to employ reasonable
20 and appropriate measures to protect against unauthorized access to confidential
21 consumer data as an unfair act or practice prohibited by Section 5 of the Federal
22 Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these
23 actions further clarify the measures businesses must take to meet their data security

24 _____
25 ³ See Federal Trade Commission, Start With Security (June 2015), available at:
26 <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>
(last visited Mar. 10, 2022).

27 ⁴ See Federal Trade Commission, Protecting Personal Information: A Guide for Business
28 (Oct. 2016), available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)
0136_proteting-personal-information.pdf (last visited Mar. 10, 2022).

⁵ See *Id.*

obligations.⁶

22. Through negligence in securing Plaintiff's and putative class members' PI and allowing access to Plaintiff's and putative class members' PI through malware, Defendant failed to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and the putative class members' PI. Accordingly, Defendant's data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

23. On December 14, 2021, Plaintiff Cindy Villanueva—a Registered Nurse—received a notice from her employer, Wellpath Recovery Solutions, LLC (“Wellpath”), alerting her that Wellpath's Kronos HR & Time Keeping Systems, operated by Defendant, was undergoing a ransomware incident affecting Kronos Private Cloud Services, causing a complete outage of Wellpath's timekeeping and payroll system. (*See* Exhibit A.) The barebones notice provided to Plaintiff only provided basic and vague information relating to the breach. As a result of the breach, Wellpath's payroll and timekeeping system was completely inoperable and unavailable, affecting all of its employee's payroll and timekeeping records. The notice also stated that the breach resulted in a disruption of “hundreds to thousands of other companies.” (*See Id.*) Significantly, Plaintiff never received legally compliant or timely notice from Defendant related to the breach, and to date, has not been informed of what type of PI is implicated in the breach.

24. As a result of the unauthorized data disclosure, Plaintiff and putative class members are now at risk for actual identity theft in addition to other forms of fraud. The ramifications of Defendant's failure to keep PI secure are long lasting and severe. Once PI is stolen, fraudulent use of that information and damage to victims may continue for years. The PI belonging to Plaintiff and class members is private, valuable, and sensitive in nature as it can be used to commit a lot of

⁶ Federal Trade Commission, Privacy and Security Enforcement Press Releases, available at <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement> (last visited Mar. 10, 2022).

1 different harms in the hands of the wrong people.

2 25. Defendant had ample resources necessary to prevent the unauthorized
3 data disclosure, but neglected to adequately implement data security measures,
4 despite its obligations to protect the PI of Plaintiff and putative class members. Had
5 Defendant remedied the deficiencies in its data security systems and adopted
6 security measures recommended by experts in the field, it would have prevented
7 the intrusions into its systems and, ultimately, the unauthorized access of PI.

8 26. As a direct and proximate result of Defendant's actions and inactions,
9 Plaintiff and putative class members have been placed at an imminent, immediate,
10 and continuing increased risk of harm from identity theft and fraud, requiring them
11 to take the time which they otherwise would have dedicated to other life demands
12 such as work and family in an effort to mitigate the actual and potential impact of
13 the unauthorized data disclosure on their lives.

14 **THE PARTIES**

15 27. Plaintiff Cindy Villanueva is a citizen and resident of the State of
16 California. Plaintiff is a licensed Registered Nurse in the State of California who
17 is employed by Wellpath Recovery Solutions, LLC. Plaintiff's employer is a client
18 of Defendant who uses its payroll and timekeeping system to process its
19 employee's payroll information. Plaintiff was impacted by the data breach and
20 ransomware attack of Defendant's payroll system that took place on or about
21 December 11, 2021, which affected her personal and sensitive information relating
22 to her payroll records.

23 28. Defendant UKG, Inc. is a corporation formed under the laws of the
24 State of Delaware, with dual corporate headquarters in Weston, Florida and Lowell,
25 Massachusetts.

26 **JURISDICTION AND VENUE**

27 29. Subject matter jurisdiction in this civil action is authorized pursuant
28 to 28 U.S.C. § 1332(d) because there are more than 100 Class Members, at least

1 one class member is a citizen of a state different from that of Defendant, and the
2 amount in controversy exceeds \$5 million, exclusive of interest and costs. The
3 court also has supplemental jurisdiction over the state law claims pursuant to 28
4 U.S.C. § 1367.

5 30. This Court has personal jurisdiction over Defendant because it
6 maintains its principal place of business in this District, is registered to conduct
7 business in California, and has sufficient minimum contacts with California.

8 31. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)
9 because a substantial part of the events or omissions giving rise to Plaintiff's and
10 putative class members' claims occurred in this District. Venue is also proper
11 under 28 U.S.C. § 1391(c) because Defendant is a corporation that does business
12 in and is subject to personal jurisdiction in this District. In addition, Plaintiff is
13 informed and believes and thereon alleges that members of the class and subclass
14 defined below reside in the Northern District. Further, pursuant to Civil L. R. 3-
15 2(c), all civil actions which arise in the counties of Alameda, Contra Costa, Del
16 Norte, Humboldt, Lake, Marin, Mendocino, Napa, San Francisco, San Mateo, or
17 Sonoma shall be assigned to the San Francisco/Oakland Divisions. A substantial
18 part of the events or omissions giving rise to the claims herein occurred also within
19 these counties and therefore assignment to the San Francisco/Oakland divisions is
20 proper.

21 CLASS ACTION ALLEGATIONS

22 32. Pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of
23 Civil Procedure, Plaintiff, individually and on behalf of all others similarly situated,
24 brings this lawsuit on behalf of herself and as a class action on behalf of the
25 following classes:

26 **Nationwide Class:** All persons in the United States whose personal
27 information was accessed, compromised, or stolen as a result of the data
28 breach announced by UKG, Inc. on or around December 11, 2021.

California Subclass: All persons in California whose personal information was accessed, compromised, or stolen as a result of the data breach announced by UKG, Inc. on or around December 11, 2021.

33. Members of the class and subclass described above will be collectively referred to as “class members.” Plaintiff reserves the right to establish other or additional subclasses, or modify any class or subclass definition, as appropriate based on investigation, discovery, and specific theories of liability.

34. Excluded from the class and subclass is Defendant and any entities in which Defendant or its subsidiaries or affiliates have a controlling interest, and Defendant’s officers, agents, and employees. Also excluded from the class are the judge assigned to this action, and any member of the judge’s immediate family.

35. **Numerosity:** The members of each class are so numerous that joinder of all members of any class would be impracticable. Plaintiff reasonably believes that class members amount to tens of millions of people. The names and addresses of class and subclass members are identifiable through documents maintained by Defendant.

36. **Commonality and Predominance:** This action involves common questions of law or fact, which predominate over any questions affecting individual Class members, including:

- (a) Whether Defendant represented to class members that it would safeguard Plaintiff’s and class members’ PI;
- (b) Whether Defendant owed a legal duty to Plaintiff and class members in exercising due care in collecting, storing, and safeguarding their PI;
- (c) Whether Defendant breached a legal duty to Plaintiff and class members to exercise due care in collecting, storing, and safeguarding their PI;
- (d) Whether Plaintiff’s and class members’ PI was accessed, compromised, or stolen in the unauthorized data disclosure;

- (e) Whether a contract existed between Plaintiff and class members, and the terms of that contract;
- (f) Whether Defendant breached the contract by having inadequate safeguards;
- (g) Whether Defendant failed to adhere to its own posted privacy policy in violation of Cal. Bus. & Prof. Code § 22576;
- (h) Whether Defendant's conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, *et seq.*;
- (i) Whether Defendant's conduct violated the Consumer Records Act, Cal. Civ. Code § 1798.80, *et seq.*;
- (j) Whether Defendant violated the California Consumer Privacy Act, Cal. Civ. Code § 1798.150, *et seq.*;
- (k) Whether Defendant's conduct violated § 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, *et eq.*;
- (l) Whether Plaintiff and class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution; and
- (m) Whether Plaintiff and class members are entitled to actual, statutory, or other forms of damages, and other monetary relief.

37. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of other similarly situated class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

38. **Typicality:** Plaintiff's claims are typical of the claims of the other class members because, among other things, Plaintiff and the other class members were injured through substantially uniform misconduct by Defendant. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other class

1 members, and there are no defenses that are unique to Plaintiff. The claims of
2 Plaintiff and those of other class members arise from the same operative facts and
3 are based on the same legal theories.

4 **39. Adequacy of Representation:** Plaintiff is an adequate representative
5 of the classes because her interests do not conflict with the interests of the other
6 class members she seeks to represent. Plaintiff has retained counsel competent and
7 experienced in complex class action litigation and Plaintiff will prosecute this
8 action vigorously. The class members' interests will be fairly and adequately
9 protected by Plaintiff and her counsel.

10 **40. Superiority:** A class action is superior to any other available means
11 for the fair and efficient adjudication of this controversy, and no unusual difficulties
12 are likely to be encountered in the management of this matter as a class action. The
13 damages, harm, or other financial detriment suffered individually by Plaintiff and
14 the other class members are relatively small compared to the burden and expense
15 that would be required to litigate their claims on an individual basis against
16 Defendant, making it impracticable for class members to individually seek redress
17 for Defendant's wrongful conduct. Even if class members could afford individual
18 litigation, the court system could not. Individualized litigation would create a
19 potential for inconsistent or contradictory judgments and increase the delay and
20 expense to all parties and the court system. By contrast, the class action device
21 presents far fewer management difficulties and provides the benefits of single
22 adjudication, economies of scale, and comprehensive supervision by a single court.

23 **FIRST CAUSE OF ACTION**

24 **Negligence**

25 **(On behalf of Plaintiff and the Nationwide Class)**

26 **41.** Plaintiff hereby re-alleges and incorporates by reference the above
27 allegations by reference as if fully set forth herein.

28 **42.** Defendant owed a duty to Plaintiff and class members to exercise

1 reasonable care in obtaining, securing, safeguarding, storing, and protecting
2 Plaintiff's and class members' PI from being compromised, lost, stolen, and
3 accessed by unauthorized persons. This duty includes, among other things,
4 designing, implementing, maintaining, and testing its data security systems to
5 ensure that Plaintiff's and class members' PI in Defendant's possession was
6 adequately secured and protected, including using encryption technologies.
7 Defendant further had a duty to implement processes that would detect their breach
8 of the payroll and timekeeping system in a timely manner.

9 43. Defendant owed a duty of care to Plaintiff and class members to
10 provide security consistent with industry standards, and to ensure that its systems
11 and networks adequately protected the PI it stored, maintained, and/or obtained.

12 44. Defendant owed a duty of care to Plaintiff and class members because
13 they were foreseeable and probable victims of any inadequate data security
14 practices. Defendant knew or should have known of the inherent risks involved in
15 allowing its payroll system to be attacked by malware and the resulting breach of
16 sensitive and valuable PI of millions of workers.

17 45. Defendant knew that the PI of Plaintiff and class members was
18 personal and sensitive payroll information that is incredibly valuable to identity
19 thieves and other criminals. Defendant also knew of the serious harms that could
20 happen if the PI of Plaintiff and class members were wrongfully disclosed, if
21 disclosure was not fixed, or if Plaintiff and class members were not provided with
22 timely and legally compliant notice detailing the PI implicated by the data breach.

23 46. Plaintiff and class members entrusted Defendant with their PI when
24 Defendant obtained their PI from their employer's for payroll services. As such,
25 Defendant had an obligation to safeguard their information and was in the best
26 position to protect against the harm suffered by Plaintiff and class members as a
27 result of the data breach to its payroll system.

28 47. Defendant's own conduct also created a foreseeable risk of harm to

1 Plaintiff's and class members' PI. Defendant's misconduct included failing to
2 implement the systems, policies, and procedures necessary to prevent the
3 unauthorized data breach.

4 48. Defendant knew, or should have known, of the risks inherent in
5 collecting and storing PI and the importance of adequate security. Defendant knew
6 about—or should have been aware of—numerous and well-publicized
7 unauthorized data disclosures affecting businesses, especially companies storing
8 sensitive financial records, such as highly valuable payroll information.

9 49. Defendant breached its duties to Plaintiff and class members by failing
10 to provide fair, reasonable, or adequate computer systems and data security to
11 safeguard the PI of Plaintiff and class members.

12 50. In addition, Defendant breached its duty to provide legally compliant
13 and timely notice of the breach to Plaintiff and class members and to adequately
14 disclose what PI was implicated by the breach as described herein and below.
15 Among other things, Defendant failed to notify Plaintiff and class members of what
16 type of PI was disclosed, accessed, stolen, or exfiltrated. Timely notice was
17 required so that Plaintiff and class members can take steps to mitigate the harms of
18 the breach by freezing their credit reports, monitoring their accounts, contacting
19 their financial institutions, obtaining credit monitoring services, and taking other
20 avenues to prevent future harms.

21 51. Defendant also had a duty to exercise reasonable care to prevent a
22 complete outage of its payroll systems, which in turn, affected millions of workers'
23 ability to receive accurate wages, timely wages, and compliant wages from their
24 employer. Defendant breached its duty by failing to remedy the breach and
25 allowing the outage to continue weeks, and even months for some workers.

26 52. Because Defendant knew that a breach of its systems would damage
27 millions of individuals whose PI was inexplicably stored or was accessible,
28 including Plaintiff and class members, Defendant had a duty to adequately protect

1 its data systems and the PI contained and/or accessible therein.

2 53. Defendant also had independent duties under state and federal laws
3 that required Defendant to reasonably safeguard Plaintiff's and class members' PI.
4 Defendant's failure to comply with state and federal regulations further evidences
5 Defendant's negligence in failing to exercise reasonable care in safeguarding and
6 protecting Plaintiff's and class members' PI.

7 54. In engaging in the negligent acts and omissions as alleged herein,
8 which permitted thieves to access Defendant's systems that stored Plaintiff's and
9 class members' PI, Defendant violated Section 5 of the FTC Act, which prohibits
10 "unfair...practices in or affecting commerce." This includes failing to have
11 adequate data security measures and failing to protect Plaintiff's and the class
12 members' PI.

13 55. Plaintiff and the class members are among the class of persons Section
14 5 of the FTC was designed to protect, and the injuries suffered by Plaintiff and the
15 class members are the types of injury Section 5 of the FTC Act was intended to
16 prevent.

17 56. Neither Plaintiff nor the other class members contributed to the
18 unauthorized data breach as described in this Complaint.

19 57. As a direct and proximate cause of Defendant's conduct, Plaintiff and
20 class members have suffered and/or will suffer injury and damages, including but
21 not limited to: (a) the loss of the opportunity to determine for themselves how their
22 PI is used; (b) the publication and/or theft of their PI; (c) out-of-pocket expenses
23 associated with the prevention, detection, and recovery from unauthorized use of
24 their PI; (d) lost opportunity costs associated with effort expended and the loss of
25 productivity addressing and attempting to mitigate the actual and future
26 consequences of the unauthorized data breach, including but not limited to efforts
27 spent researching how to prevent, detect, contest and recover from tax fraud and
28 identity theft; (e) costs associated with placing freezes on credit reports; (f) anxiety,

1 emotional distress, loss of privacy, and other economic and non-economic losses;
2 (g) the continued risk to their PI, which remains in Defendant's possession (and/or
3 Defendant has access to) and is subject to further unauthorized disclosures so long
4 as Defendant fails to undertake appropriate and adequate measures to protect the
5 PI in its continued possession; and, (h) future costs in terms of time, effort, and
6 money that will be expended to prevent, detect, contest, and repair the inevitable
7 and continuing consequences of compromised PI.

8 58. But for Defendant's wrongful and negligent breach of their duties
9 owed to Plaintiff and class members, their PI would not have been compromised,
10 stolen, and viewed by unauthorized persons. Defendant's negligence was a direct
11 and legal cause of the theft of the PI of Plaintiff and class members and all resulting
12 damages.

13 59. The injury and harm suffered by Plaintiff and class members was the
14 reasonably foreseeable result of Defendant's failure to exercise reasonable care in
15 safeguarding and protecting Plaintiff's and the other class members' PI.

16 60. As a result of this misconduct by Defendant, the PI and financial
17 information of Plaintiff and class members was compromised, placing them at a
18 greater risk of identity theft, subjecting them to identity theft, and resulting in
19 disclosure of their PI to third parties without their consent. Plaintiff and class
20 members also suffered diminution in value of their PI in that it is now easily
21 available to hackers on the dark web.

22 61. As a direct and proximate result of Defendant's negligence, Plaintiff
23 and class members have been injured as described herein, and are entitled to
24 damages including, but not limited to, compensatory, nominal, and consequential
25 damages.

26 ///

27 ///

28 ///

SECOND CAUSE OF ACTION

Breach of Contract

(On behalf of Plaintiff and the Nationwide Class)

62. Plaintiff hereby re-alleges and incorporates by reference the above allegations by reference as if fully set forth herein.

63. At all relevant times a contract existed and was in force between Defendant on one hand and Plaintiff and the class members on the other. This contract was written and was supplemented by implied and written terms that existed and were maintained online on Defendant's website. Any implied contracts or supplemental terms or conditions of the contract were written by Defendant and published electronically to Plaintiff and the class members online in such a manner and through such conduct so as to create promises on the part of the Defendant.

64. These written conditions include, but are not limited to the terms and conditions included in its security section of Defendant's Privacy Notice, which states the following:

"To prevent unauthorized access or disclosure, to maintain data accuracy, and to allow only the appropriate use of your PI, UKG utilizes physical, technical, and administrative controls and procedures to safeguard the information we collect.

To protect the confidentiality, integrity, availability and resilience of your PI, we utilize a variety of physical and logical access controls, firewalls, intrusion detection/prevention systems, network and database monitoring, anti-virus, and backup systems. We use encrypted sessions when collecting or transferring sensitive data through our websites.

We limit access to your PI and data to those persons who have a specific business purpose for maintaining and processing such information. Our employees who have been granted access to your PI are made aware of their responsibilities to protect the confidentiality, integrity, and availability of that information and have been provided training and instruction on how to do so."⁷

⁷ Privacy Notice, Security, UKG, <https://www.ukg.com/privacy#4243725865-507775231> (last visited Mar. 10, 2022).

1 65. Defendant's privacy policy is an agreement between Defendant and
2 its customers and the end-users including Plaintiff and class members who
3 entrusted Defendant with their PI, including sensitive payroll information and
4 records. Defendant breached its own privacy policy by allowing Plaintiff's and
5 class members' PI to be accessed to persons who do not have a "specific business
6 purpose" for accessing their PI.

7 66. Defendant also breached these duties and violated these promises by
8 failing to properly safeguard the sensitive personal and financial information of
9 Plaintiff and class members by failing to use the promised safeguards, and by
10 failing to use security measures that comply with federal laws including but not
11 limited to Section 5(a) of the FTC Act, by failing to protect customer records and
12 information from threats, hazards, or unauthorized access, by negligently,
13 carelessly, and recklessly collecting, maintaining, and controlling this information,
14 and by engineering, designing, maintaining, and controlling systems that exposed
15 their end-users' sensitive personal and financial information of which Defendant
16 had possession to control the risk of exposure to unauthorized persons.

17 67. Defendant violated their commitment to maintain the confidentiality
18 and security of the PI of Plaintiff and class members by failing to comply with
19 applicable laws, regulations, and industry standards relating to data security.

20 68. At all relevant times and in all relevant ways, Plaintiff and class
21 members performed their obligations under the contract in question or were
22 excused from performance of such obligations through the unknown and
23 unforeseen conduct of others.

24 69. As a direct consequence of the breaches of contract and violations of
25 promises described above, unauthorized users gained access to, exfiltrated, stole,
26 and gained disclosure of the sensitive personal and financial information of
27 Plaintiff and class members, causing them harms and losses including but not
28 limited to (a) economic loss including from unauthorized charges, (b) the loss of

control over the use of their identity, (c) harm to their constitutional right to privacy, (d) lost time dedicated to the investigation of the breach of their own personal information, (e) costs associated with the detection and prevention to cure any harm to their privacy including credit freezes, credit monitoring, and identity theft services, (e) the need for future expenses and time dedicated to the recovery and protection of further loss associated with the continued risk of exposure of their PI, (f) loss of wages stemming from the complete outage of their payroll and timekeeping records, (g) the diminution of value of their PI, (h) and privacy injuries associated with having their sensitive personal and financial information disclosed.

70. Plaintiff and class members were harmed as a result of Defendant's breach because their PI and financial information stemming from their sensitive payroll records was compromised, placing them at a greater risk of identity theft and subjecting them to identity theft. Plaintiff and class members also suffered diminution of value of their PI in that it is now easily available to hackers on the dark web. Plaintiff and class members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

71. Plaintiff and class members are entitled to compensatory, consequential, and nominal damages resulting from Defendant's breach of contract.

THIRD CAUSE OF ACTION

Violation of the California Consumer Privacy Act ("CCPA")

(Cal. Civ. Code § 1798.150)

(On behalf of Plaintiff and the California Subclass)

72. Plaintiff hereby re-alleges and incorporates by reference the above allegations by reference as if fully set forth herein.

73. The CCPA creates a private right of action for violations of the statute

1 as specified under Cal. Civ. Code § 1798.150(a)(1), which states:

2 Any consumer whose nonencrypted and nonredacted personal information,
3 as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section
4 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or
5 disclosure as a result of the business's violation of the duty to implement and
6 maintain reasonable security procedures and practices appropriate to the
7 nature of the information to protect the personal information may institute a
8 civil action for any of the following:

9 (A) To recover damages in an amount not less than one hundred dollars
10 (\$100) and not greater than seven hundred and fifty (\$750) per consumer
11 per incident or actual damages, whichever is greater.

12 (B) Injunctive or declaratory relief.

13 (C) Any other relief the court deems proper.

14 74. At all relevant times, Defendant was and still is a "business" under
15 Section 1798.140(b) of the CCPA as a corporation operating in the State of
16 California that collect consumers' personal information, and that either has annual
17 operating revenue above \$25 million, collects the personal information of 50,000
18 or more California residents annually, or derives at least 50 percent of its annual
19 revenue from the sale of personal information of California residents.

20 75. At all relevant times, Plaintiff and the California subclass were
21 "consumers" under Section 1798.140(g), and also, under the terms of the CCPA as
22 natural persons as defined in Section 17014 of Title 18 of the California Code of
23 Regulations.

24 76. By the acts described above, Defendant violated the CCPA by
25 negligently, carelessly, and recklessly collecting, maintaining, and controlling
26 Plaintiff's and class members' sensitive personal and financial information and by
27 engineering, designing, maintaining, and controlling systems that exposed
28 Plaintiff's and class members' sensitive personal and financial information of

1 which Defendant had possession to control the risk of exposure to unauthorized
 2 persons, thereby violating their duty to implement and maintain reasonable security
 3 procedures and practices appropriate to the nature of the information to protect the
 4 personal information. Defendant allowed unauthorized users to view, use,
 5 manipulate, exfiltrate, and steal the nonencrypted and nonredacted personal
 6 information of Plaintiff and class members, including their personal and financial
 7 payroll information.

8 77. Section 1798.150(b) specifically provides that: “No notice shall be
 9 required prior to an individual consumer initiating an action solely for actual
 10 pecuniary damages suffered as a result of the alleged violations of this title.”
 11 Plaintiff has issued the required notice of these alleged violations to Defendant
 12 under Section 1798.150(b) and will be amending this Complaint to seek statutory
 13 and injunctive relief upon the expiration of the 30-day cure period pursuant to
 14 Section § 1798.150(a). Accordingly, by way of this Complaint, Plaintiff seeks
 15 actual pecuniary damages suffered as a result of the violations of the California
 16 Consumer Privacy Act on behalf of herself and similarly situated putative class
 17 members.

18 78. As a result of Defendant’s violations, Plaintiff and the class members
 19 are entitled to all actual and compensatory damages according to proof or statutory
 20 damages allowable under the CCPA, whichever are higher, and to such other and
 21 further relief as this Court may deem just and proper.

22 **FOURTH CAUSE OF ACTION**

23 **Violation of the California Customer Records Act (“CRA”)**

24 **(Cal. Civ. Code § 1798.80 *et seq.*)**

25 **(On behalf of Plaintiff and the California Subclass)**

26 79. Plaintiff hereby re-alleges and incorporates by reference the above
 27 allegations by reference as if fully set forth herein.

28 80. California Civil Code section 1798.80, *et seq.*, known as the

1 “Customer Records Act” (“CRA”) was enacted to “encourage business that own,
2 license, or maintain personal information about Californians to provide reasonable
3 security for that information.” Cal. Civ. Code § 1798.81.5(a)(1).

4 81. Section 1798.81.5(b) of the CRA requires any business that “owns,
5 licenses, or maintains personal information about a California resident” to
6 “implement and maintain reasonable security procedures and practices appropriate
7 to the nature of the information,” and “to protect the personal information from
8 unauthorized access, destruction, use, modification, or disclosure.”

9 82. Section 1798.81.5(d)(1)(B) defines “personal information” as
10 including an individual’s first name or first initial and the individual’s last name in
11 combination with any one or more of the following data elements, when either the
12 name or the data elements are not encrypted or redacted: (i) social security number,
13 (ii) driver’s license number, California identification card number, tax
14 identification number, passport number, military identification number, or other
15 unique identification number issued on a government document commonly used to
16 verify the identity of a specific individual, (iii) account number or credit or debit
17 card number, in combination with any required security code, access code, or
18 password that would permit access to an individual’s financial account, (iv)
19 medical information, (v) health insurance information, (vi) unique biometric data
20 generated from measurements or technical analysis of human body characteristics,
21 such as a fingerprint, retina, or iris image, used to authenticate a specific individual,
22 (vii) genetic data. Cal. Civ. Code § 1798.81.5(d)(1)(A).

23 83. Personal information also includes “[a] username or email address in
24 combination with a password or security question and answer that would permit
25 access to an online account.” Cal. Civ. Code § 1798.81.5(d)(1)(B).

26 84. At all relevant times, Defendant was and still is a “business” under the
27 terms of the CRA as sole proprietorships, partnerships, corporations, associations,
28 financial institutions, or other groups, operating in the State of California that

1 owned or licensed computerized data that included the personal information of
2 Plaintiff and the California subclass.

3 85. At all relevant times, Plaintiff and the California subclass were
4 “customers” under the terms of the CRA as natural persons who provided personal
5 information to Defendant for the purpose of obtaining a service from Defendant.

6 86. As alleged in detail above, Defendant failed to “implement and
7 maintain reasonable security procedures and practices appropriate to the nature of
8 the information,” and “to protect the personal information from unauthorized
9 access, destruction, use, modification, or disclosure,” resulting in the massive
10 breach at issue in this complaint that occurred on or around December 11, 2021.

11 87. By the acts described above, Defendant violated the CRA by allowing
12 unauthorized access to Plaintiff’s and class members’ personal and financial
13 information, including highly sensitive payroll information.

14 88. Moreover, the statute further provides: “A person or business that
15 maintains computerized data that includes personal information that the person or
16 business does not own shall notify the owner or licensee of the information of the
17 breach of the security of the data immediately following discovery, if the personal
18 information was, or is reasonably believed to have been, acquired by an
19 unauthorized person.” Cal. Civ. Code § 1798.82.

20 89. Any person or business that is required to issue a security breach
21 notification under the CRA must meet the following requirements under Section
22 1798.82(d).

23 (a) The name and contact information of the reporting person or business
24 subject to this section;

25 (b) A list of the types of personal information that were or are reasonably
26 believed to have been the subject of a breach;

27 (c) If the information is possible to determine at the time the notice is
28 provided, then any of the following:

- i. the date of the breach,
- ii. the estimated date of the breach, or
- iii. the date range within which the breach occurred. The notification shall also include the date of the notice;

(d) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

(e) A general description of the breach incident, if that information is possible to determine at the time the notice is provided;

(f) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number;

(g) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

90. Defendant failed to provide the legally compliant notice under Section 1798.82(d) to Plaintiff and members of the California subclass, including among other things, the types of personal information that were or are reasonably believed to have been the subject of a breach. Defendant learned of the breach on or about December 11, 2021. Plaintiff and class members were entitled to receive timely notice from Defendant, but instead, found out about the breach of their payroll information from their employer or through news and media outlets. As a result, Defendant has violated Section 1798.82 by not providing legally compliant and timely notice directly to Plaintiff and class members.

1 91. Plaintiff, and on information and belief, many class members affected
2 by the breach, have not received any notice at all from Defendant in violation of
3 Section 1798.82(d).

4 92. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiff and
5 class members suffered incrementally increased damages separate and distinct
6 from those simply caused by the breaches themselves.

7 93. As a direct consequence of the actions as identified above, Plaintiff
8 and class members incurred additional losses and suffered further harm to their
9 privacy, including but not limited to economic loss, the loss of control over the use
10 of their identity, harm to their constitutional right to privacy, lost time dedicated to
11 the investigation of the breach and effort to cure any resulting harm, the need for
12 future expenses and time dedicated to the recovery and protection of further loss,
13 and privacy injuries associated with having their sensitive personal, financial, and
14 payroll information disclosed, that they would not have otherwise incurred but for
15 the data breach of Defendant's payroll systems.

16 94. As a direct result of Defendant's violation of the California Customer
17 Records Act, Plaintiff and class members were harmed because their PI and
18 financial information stemming from their sensitive payroll records was
19 compromised, placing them at a greater risk of identity theft and subjecting them
20 to identity theft. Plaintiff and class members also suffered diminution of value of
21 their PI in that it is now easily available to hackers on the dark web. Plaintiff and
22 class members have also suffered consequential out of pocket losses for procuring
23 credit freeze or protection services, identity theft monitoring, and other expenses
24 relating to identity theft losses or protective measures.

25 95. Cal. Civ. Code § 1798.84(b) provides that "[a]ny customer injured as
26 a result of violating the CRA may institute a civil action to recover damages."

27 96. As a result of Defendant's violations, Plaintiff and class members are
28 entitled to all actual and compensatory damages according to proof, and to non-

1 economic injunctive relief allowable under the CRA, and to such other and further
2 relief as this Court may deem proper.

3 **FIFTH CAUSE OF ACTION**

4 **Violation of the California Constitution's Right to Privacy**

5 **(California Constitution, Article I, Section 1)**

6 **(On behalf of Plaintiff and the California Subclass)**

7 97. Plaintiff hereby re-alleges and incorporates by reference the above
8 allegations by reference as if fully set forth herein.

9 98. The California Constitution provides: "All people are by nature free
10 and independent and have inalienable rights. Among these are enjoying and
11 defending life and liberty, acquiring, possessing, and protecting property, and
12 pursuing and obtaining safety, happiness, and privacy." (Cal. Const., art. I, § 1.)

13 99. The right to privacy in California's constitution creates a private right
14 of action against private and government entities. Indeed, "[t]he California
15 Constitution creates a private right that protects individuals from intrusions by
16 private parties." *In re Google Location History Litigation*, 428 F. Supp. 3d 185,
17 196 (N.D. Cal. Dec. 19, 2019).

18 100. Plaintiff and the California subclass have a legally recognized and
19 protected privacy interest in their personal, financial, and payroll information
20 provided to and obtained by Defendant, including but not limited to an interest in
21 precluding the dissemination or misuse of this sensitive and confidential
22 information and the misuse of this information for malicious purposes such as the
23 theft of funds and property.

24 101. Plaintiff and class members reasonably expected Defendant would
25 prevent the unauthorized viewing, use, manipulation, exfiltration, theft, and
26 disclosure of their personal and financial information and the unauthorized use of
27 their accounts.

28 102. Defendant's conduct described herein resulted in a serious invasion of

1 the privacy of Plaintiff and the California subclass, as the release of personal and
 2 financial information, such as the sensitive information Defendant stored in its
 3 payroll system could highly offend a reasonable individual. Indeed, the
 4 unauthorized access of Plaintiff's and class members' personal and financial
 5 information implicated by Defendant's breach rises to the requisite level of an
 6 egregious breach of social norms for purposes of establishing an invasion of
 7 privacy.

8 103. As a direct consequence of the actions as identified above, Plaintiff
 9 and class members incurred additional losses and suffered further harm to their
 10 privacy, including but not limited to economic loss, the loss of control over the use
 11 of their identity, harm to their constitutional right to privacy, lost time dedicated to
 12 the investigation of the breach and effort to cure any resulting harm, the need for
 13 future expenses and time dedicated to the recovery and protection of further loss,
 14 and privacy injuries associated with having their sensitive personal, financial, and
 15 payroll information disclosed, that they would not have otherwise incurred but for
 16 the data breach of Defendant's payroll system.

17 **SIXTH CAUSE OF ACTION**

18 **Violation of the Unfair Competition Law ("UCL")**

19 **(Cal. Bus. Prof. Code § 17200, *et seq.*)**

20 **(On behalf of Plaintiff and the California Subclass)**

21 104. Plaintiff hereby re-alleges and incorporates by reference the above
 22 allegations by reference as if fully set forth herein.

23 105. By reason of the conduct alleged herein, Defendant engaged in
 24 unlawful practices within the meaning of the UCL. The conduct alleged herein is
 25 a "business practice" within the meaning of the UCL.

26 106. By engaging in the above-described unfair business acts and practices,
 27 Defendant committed and continues to commit one or more acts of unlawful,
 28 unfair, and fraudulent conduct within the meaning of the UCL. These acts and

1 practices constitute a continuing and ongoing unlawful business activity, as defined
2 by the UCL, and justify the issuance of an injunction and any other equitable relief
3 pursuant to the UCL.

4 107. Plaintiff and class members were entitled to assume, and did assume,
5 that Defendant would take appropriate measures to keep their PI and safe.
6 Defendant did not disclose at any time that Plaintiff's and class members' PI was
7 vulnerable to hackers because Defendant's data security measures were inadequate.

8 108. Defendant violated the UCL by misrepresenting, both by affirmative
9 conduct and by omission, the safety of its payroll and timekeeping system, Kronos
10 Private Cloud, specifically the security thereof, and their ability to safely store
11 Plaintiff's and class members' PI and sensitive payroll information. Defendant also
12 violated the UCL by failing to implement reasonable and appropriate security
13 measures or follow industry standards for data security, failing to comply with its
14 own posted privacy policies, and by failing to provide legally compliant notice to
15 Plaintiff and class members detailing the full implication of the breach, as required
16 by the California Consumer Records Act.

17 109. Defendant's acts, omissions, and misrepresentations as alleged herein
18 were unlawful and in violation of, *inter alia*, Cal. Civ. Code § 1798.81.5(b), Section
19 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), and Cal. Bus. & Prof.
20 Code § 22576 (as a result of Defendant failing to comply with its own posted
21 privacy policies).

22 110. Defendant engaged in unfair business practices under the "balancing
23 test." The harm caused by Defendant's actions and omissions, as described in
24 detail above, greatly outweigh any perceived utility. Indeed, none of Defendant's
25 actions or inactions can be said to have had any utility at all. Defendant's failures
26 were clearly injurious to Plaintiff and class members, directly causing the harms
27 alleged below.

28 111. Defendant also engaged in unfair business practices under the

1 “tethering test.” Defendant’s actions and omissions, as described in detail above,
 2 violated fundamental public policies expressed by the California Legislature. *See*,
 3 *e.g.*, Cal. Civ. Code § 1798.1 (“The Legislature declares that . . . all individuals
 4 have a right of privacy in information pertaining to them The increasing use
 5 of computers . . . has greatly magnified the potential risk to individual privacy that
 6 can occur from the maintenance of personal information.”); Cal. Civ. Code §
 7 1798.81.5(a) (“It is the intent of the Legislature to ensure that personal information
 8 about California residents is protected.”) Indeed, Defendant’s acts and omissions
 9 thus amount to a clear violation of the law.

10 112. Defendant also engaged in unfair business practices under the “FTC
 11 test.” The harm caused by Defendant’s actions and omissions, as described in
 12 detail above, is substantial in that it has affected millions of class members and has
 13 caused those persons to suffer actual harms. Such harms include a substantial risk
 14 of identity theft, disclosure of Plaintiff’s and class members’ PI to third parties
 15 without their consent, diminution in value of their PI, consequential out of pocket
 16 losses for procuring credit freeze or protection services, identity theft monitoring,
 17 and other expenses relating to identity theft losses or protective measures. This
 18 harm continues given the fact that Plaintiff’s and class members’ PI remains in
 19 Defendant’s possession, without adequate protection, and is also in the hands of
 20 those who obtained it without their consent. Defendant’s actions and omissions
 21 also violated Section 5(a) of the Federal Trade Commission Act. *See In re LabMD,*
 22 *Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to
 23 employ reasonable and appropriate measures to secure personal information
 24 collected violated § 5(a) of FTC Act).

25 113. Defendant’s acts and practices constitute a continuing and ongoing
 26 unlawful business activity defined by the UCL. In particular, Defendant failed and
 27 continues to fail to implement and maintain reasonable security procedures and
 28 practices appropriate to protect the PI, failed and continues to fail to inform Plaintiff

1 and class members of the full implications of the breach of their PI, and made and
2 continues to make misrepresentations to customers regarding the nature and quality
3 of their data protection, all in violation of, *inter alia*, the following California laws:

4 (a) Negligence as defined in California Civil Code section 1714;

5 (b) California Civil Code section 1798.81.5(b);

6 (c) California Civil Code section 1798.82(a);

7 (d) California Civil Code section 1798.150(a);

8 (e) Cal. Bus. & Prof. Code § 22576; and

9 (f) California Constitution, Article I, Section 1.

10 114. Defendant's conduct is contrary to the public welfare as it transgresses
11 civil statutes of the State of California designed to protect individuals'
12 constitutional and statutory right to privacy, violates established public policy, and
13 has been pursued to attain an unjustified monetary advantage for Defendant by
14 creating personal disadvantage and hardship to Plaintiff and class members. As
15 such, Defendant's business practices and acts have been immoral, unethical,
16 oppressive, and unscrupulous and have caused injury to Plaintiff and class
17 members far greater than any alleged countervailing benefit.

18 115. Defendant made and continues to make the representations set forth
19 above, including but not limited to specific representations in their privacy policy
20 regarding the nature and quality of their data security and their representations that
21 they limit access Plaintiff's and class members' PI only to those who have a specific
22 business purpose for maintaining and processing such information. These false
23 representations were, and continue to be made, likely to deceive the public and
24 reasonable consumers. Defendant, at all times when it made these representations,
25 knew them to be false and intended to, and did, induce reliance upon these false
26 representations by Plaintiff and class members, who reasonably relied upon the
27 aforementioned statements and representations and, as a consequence, suffered
28 economic harms and losses.

116. As a direct and proximate consequence of the actions as identified above, Plaintiff and class members suffered and continue to suffer harms and losses including but not limited to economic loss, the loss of control over the use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and attempts to cure any harm to their privacy, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal and financial information disclosed.

117. In addition, Plaintiff's and class members' PI was taken and is in the hands of those who will use it for their own advantage, or will sell it for value, making it clear that the hacked information is of tangible value. Plaintiff and class members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

118. Plaintiff seeks an order of this Court awarding injunctive relief and any other relief allowed under the UCL, including interest and attorneys' fees pursuant to, *inter alia*, Code of Civil Procedure section 1021.5, and to such other and further relief as this Court may deem just and proper.

PRAYER FOR RELIEF

Plaintiff, on her own behalf and on behalf of all others similarly situated, prays for relief and judgment against Defendant, as follows:

1. For an order certifying the proposed Class and Subclass pursuant to Federal Rules of Civil Procedure, Rule 23;

2. For an order appointing Plaintiff, Cindy Villanueva, as class representative.

3. For appointment of Lebe Law, APLC as class counsel for all purposes;

4. For an order enjoining Defendant, its affiliates, successors,

transferees, assignees, and the officers, directors, partners, agents, and employees thereof, and all other persons acting or claiming to act on their behalf or in concert with them, from continuing the unlawful practices as set forth herein, including but not limited to employing substandard data safety protocols to protect Plaintiff's and class members' payroll information and PI.

5. Requiring Defendant to provide appropriate credit monitoring services to Plaintiff and class members;

6. For actual, compensatory, consequential, and nominal damages according to proof pursuant to the California Civil Code and all other applicable laws and regulations;

7. For civil and statutory penalties available under applicable law;

8. For pre-judgment and post-judgment interest;

9. Finding that Defendant's conduct was negligent, unfair, and unlawful business practices as alleged herein;

10. Enjoining Defendant from engaging in further negligent, unfair, and unlawful business practices alleged herein;

11. For an award of attorneys' fees, costs, and expenses as authorized by applicable law; and

12. For such other and further relief as this Court may deem just and proper.

Dated: March 21, 2022

LEBE LAW, APLC

By: /s/ Jonathan M. Lebe

Jonathan M. Lebe

Zachary T. Gershman

Nicolas W. Tomas

Attorneys for Plaintiff Cindy Villanueva,
individually and on behalf of all others
similarly situated

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all claims so triable.

Dated: March 21, 2022

LEBE LAW, APLC

By: /s/ Jonathan M. Lebe
Jonathan M. Lebe
Zachary T. Gershman
Nicolas W. Tomas
Attorneys for Plaintiff Cindy Villanueva,
individually and on behalf of all others
similarly situated

EXHIBIT A

Urgent: Kronos Cybersecurity Incident

Wellpath Communications <Communications@Wellpath.us>

Tue 12/14/2021 10:18 AM

To: Craig Diamond <craig.diamond@wellpath.us>

Email Priority: Urgent

Read Immediately

Urgent: Kronos Cybersecurity Incident

To: All Wellpath Team Members

From: Wellpath Cybersecurity Team

Wellpath Team Members,

As you may have seen in the news, UKG Kronos, Wellpath's Kronos HR & Time Keeping Systems partner, is undergoing a ransomware incident affecting Kronos Private Cloud Services, which is the host for Wellpath's timekeeping system. These systems have been unavailable since Saturday night 12/11. **Here is the communication from UKG Kronos.**

This means Wellpath Kronos HR & Time Keeping Systems are completely inoperable and unavailable which affects the way you will enter time, request PTO, and more.

Our most important priorities are to pay you accurately and timely, and ensure your personal data is secure.

Key Information:

- At this time there is no indication that any personal individual data has been extracted from the environments.
- This is a global outage which impacts a number of UKG/Kronos data centers and customers. Wellpath was disrupted along with hundreds to thousands of other companies.
- UKG/Kronos has communicated it could take weeks to get the systems back online.
- You will be paid during this incident. Our teams are working on solutions to ensure your pay is accurate and timely.
- In the next few days more information will be forthcoming regarding interim manual processes. In the meantime:
 - If you swipe in and out at a time clock, continue to do so until further notice.
 - Work with your supervisor on manual recording of time-keeping, PTO requests, and other HR related requests.

Wellpath has established a multi-departmental team that is developing the processes and procedures required to ensure

that all Wellpath Team Members continue to get paid in a timely and accurate fashion. The interim processes, such as manual time tracking, will create some extra work for our Team Members, but are required to ensure everyone is paid accurately.

Please be on the lookout for additional updates and instructions from Wellpath Communications and your leaders.

Questions & Comments:

Please direct questions to your manager.